REMARKS

Reconsideration and allowance of the above-referenced application are respectfully requested.

Initially, in response to the "response to arguments" set forth in section 1.2 of the Official Action, the undersigned notes that claims 1 and 6 already recited that the first communication part had "its access controlled by requiring users of the first communication part to use a first... key". However, since applicant agrees that the intent of this claim is to prevent access to those who do not have the first key, this has been made more explicit in claims 1 and 6, thereby obviating the rejection.

In addition, the rejection states that Stewart's "SSIDs" are the same as the recited "keys". This contention is respectfully traversed. The rejection requires "proof of how the system IDs and Stewart are not keys". In response, applicant supplies a paper from "Network World" found on the Internet, and purportedly dated May 1, 2002. According to this document, the system ID, also called SSID, is the lowest level of security. This just identifies the network and is not a "key that controls access".

In order to emphasize this distinction, the claims are amended to recite that the "key" is used to control access.

As such, being the lowest level of security that is broadcast to identify the networks that can be selected. This is not a "key" that can be used to control access, as described herein. Moreover, this article makes it clear that SSIDs were never intended to be a key that controls access. In order to make this clear in certain claims, the term "key" has been changed to "key which controls access".

The original specification clearly did refer to the concept of a key that is known to everyone in a key that is not known to everyone, the public key in box 110 in figure 1, and the other key that is not public in box 100 in figure 1. In order to obviate the rejection based on the word "secret" this has been changed herein to -nonpublic--.

With regards the three layers of access, Stewart does not disclose this, as will be described in further detail herein.

Claims 1-12, 14 and 7-23 stand rejected under 35 USC 112, first paragraph as allegedly failing to comply with the written description requirement. On page 4, the rejection states that there is no support for the two separate communication streams as claims. This contention is respectfully traversed. Looking simply at figure 1, once these three separate NICs, 100, 110, 120, each transmitting a separate communication stream.

With regard the questions and objections regarding the communication parts and the communication streams, applicant believe that the objections are based on a misunderstanding by

the patent office of the intent of these claims. See for example figure 1 that shows three separate network cards or NICs 100, 110, 120. Each NIC is within the housing 130, and hence in the same area. Each of them also transmit a separate communication stream. The NIC 100 is shown transmitting the first wireless stream that says "full file access". The second NIC 110 is shown communicating a second wireless stream showing "print and Internet only". The third NIC is shown transmitting a third wireless stream. These are separate streams.

Hence, the first communication part and the second communication part transmit two separate communication streams. The first stream is the first stream from the first NIC 100, the second stream is the second stream from the second NIC 110.

Both of these streams are transmitted "over substantially as same transmitting area", since they are transmitted from network cards that are right next to each other, in the same housing and hence have an overlapping area. At least part of the range of communications would overlap.

Hence, in response to the examiner's comments that this is not what applicants intend, with all due respect this is precisely what is intended by these claims. The fact that the patent office has misunderstood this, is one powerful indicia of its non obviousness.

The next objection is that there is no support for providing automatic access to users that have the first access key. This

contention is further respectfully traversed, since page 3 lines 7-13 describes that users are given an encryption key and this encryption key provides them with access to resources. While applicants agree that the specific implementation details of this access is not given in the specification. However, the specification does describe existing software that can be used to implement this -- the last line on page 3 describes using Windows XP as the operating system. Windows XP provides automatic control of access and encryption keys, via 801.11 communication protocols (see page 3 line 6). Clearly, therefore, this disclosure enables one having ordinary skill in the art to practice this subject matter, since the details of access would have been automatically handled by the operating system.

The term "secret key" has been changed to "nonpublic key". It is clear in context that the encryption key described on page 3 as being ABC DEF is a nonpublic key, as compared with the encryption key called “public” described on page 4. Clearly, therefore, there is support for this feature.

Claim 21 describes the automatically granting. Note that this was the subject matter of original claim 21 which is hence part of the specification as originally filed. This is also automatically handled by Windows XP.

With regard to the question about automatic access, again this is conventional within the XP operating system, described at the bottom of page 3. Page 3, line third from the bottom,

explains that the "amount of access... may be assigned by the operating system which drives the NICs". Applicant believes that it is not necessary to describe the details of how to interface with a system such as this which is controlled solely by the operating system. When you operate a NIC in a computer, you do not need to describe the specific implementation details of operating that NIC, since the operating system automatically handles it.

Claims 1-12, 14 and 17-23 stand rejected under 35 USC 112, second paragraph, as allegedly being indefinite. In response, these claims are amended herewith for definiteness.

The "communication stream" is believed completely clear in context.

The antecedent in claim 5 has been corrected.

The antecedent basis in claims 7 and 8 has been corrected.

Claim 6 has been amended but has not removed the word "first" since claim 12 now recites a "second" encryption key.

The antecedent issue in claim 10 has been corrected.

The antecedent issue in claim 14 has been corrected.

The antecedent issue in claim 22 has been corrected.

A "second subset" has been added to claim 17 to obviate the issue.

The antecedent issue in the preamble of claims 2-5 has been corrected.

A new figure 1 will be provided in due course.

Claims 1, 3, 5-8, 10, 13, 15 and 16 stand rejected under 35 USC 102(e) as allegedly being anticipated by Stewart. Claims 2,4 and 17-23 stand rejected over Stewart in view of Chen. Each of these contentions, however, are respectfully traversed for reasons set forth herein.

Stewart teaches a system where a number of different users can receive access to the Internet, and can receive different levels of access. According to one embodiment described by Stewart, user identification is used to determine which of the different levels of access are provided. A number of different embodiments are also disclosed by Stewart.

The embodiment bridging columns 9-10 discloses use of multiple different quality of service metrics. There are a number of different access points on the system. The embodiment at the bottom of column 10 allows selecting which of a plurality of different access points to use. The system ID is used to carry out the selecting. column 11 lines 17-33 suggests that the different system IDs may prove correspond to different network providers. Column 13 describes that the privilege level indicates which network resources the user may access, and that one of these privilege levels only allow certain access to resources.

The present application, however, discloses, and now claims, a very different kind of system. An important feature, now defined by claim 1, recites that there are different and separate communication parts and that the access to these parts is controlled by different keys. Moreover, as claimed, these different communication parts are formed by "separate communication stream[s] … over substantially a same transmitting area" .

This substantially simplifies the system, and makes it easier to obtain access. More specifically, claim 1 defines a first communication part defining a first class of service that includes access to files and a second communication part that transmits a separate communication stream over substantially the same area and defines a second class of service. The first communication part is accessed by using a non-public key and automatically provides access to users that have the non-public key. The second communication part allows access without the non-public key.

In this way, communications and the amount of access is easily controlled: simply by determining whether the user has, or does not have, the non-public key. Moreover, one NIC can transmit a first stream that has certain characteristics, that anyone with the non-public key can access. Another NIC can transmit the other stream.

Stewart is much more complicated, since it requires that the user credentials be checked and verified. While Stewart does allow access based on SSID, it does not disclose the now claimed subject matter of automatically allowing access based on possessing a non-public key of a type that controls access as claimed. SSIDs are not secret keys, as claimed. See the evidence attached.

Claim 1 also defines sets of permissions, where one of the sets of permission comprises access to files, where the user is granted access to the files when they have the encryption key but not granted access to the files when they do not have the encryption key. The rejection states that Stewart's column 14 and 16 disclose this subject matter. However, the cited section of column 14 merely discloses private portions on the network. The cited section of column 16 again describes that different computing resources can be stored on the network. It does not disclose that users with an encryption key can access files on the network, but users who do not have the encryption key cannot access those files as defined by claim 1.
Moreover, nothing in Stewart shows or discloses the "separate communication stream[s] … over substantially a same transmitting area" .

Therefore, claim 1 is not anticipated by Stewart.

Claim 3 defines a third communication part, defining a third class of service with third sets of permissions. This third set

of permissions allows access to only specified Internet site. Therefore, collectively, claim 3 allows three different sets of permissions: the highest level of permission, the second level of permission which does not provide access to files, and the third level of permission which provides access to only specified Internet sites. Nothing in Stewart suggests such a system with three layers of access.

Claim 5 defines even further patentable details, where the first and second levels are based on secret keys, and the third level is granted when no key is available. This further simplifies the access granting mechanism.

Claim 6 has been amended to recite that access is automatically granted to users having the first non-public key, and that the second wireless network portion can be accessed by users not having the non-public key. This claim should be allowable along with the claims which depend therefrom.

Claim 7 specifies an amount of bandwidth.

Claim 9 defines that there are separate wireless network interface cards operating in the same location forming the different networks. This is not disclosed by Stewart.

Claim 10 defines the third layer of network access. Stewart does not disclose this.

Claim 11 defines that the key is an encryption key, which is not disclosed or suggested by the cited prior art. The SSID is certainly not an encryption key.

Claim 13 defines different levels of access based on different possessions of encryption keys. This is not disclosed by the prior art.

Note that these advantages are not disclosed or contemplated by the prior art, and certainly not obvious based thereon. Nothing in the prior art suggests the advantage of automatically granting access based on the possession of a secret key as in claim 1 and others. Nothing in the prior art teaches multiple different networks, each having a different capability, and one of which can be accessed depending on which of the keys is obtained as in claim 3 and others. Different ones of the claims define different aspects of the above, and the advantages of this are not recognized by the prior art. Therefore, these claims should be allowable for these reasons.

The remaining depending claims are rejected based on Stewart in view of Chen. Chen shows dynamic provisioning of DSL services, which allows, in at least one embodiment, charging per access. However, even if this rejection is correct, these claims should be allowable by virtue of their dependency.

Finally, this amendment should be entered after final, since many of the changes made herein are responsive to the Examiner's requests, and because this places the case in better condition for appeal.

It is believed that all of the pending claims have been addressed in this paper. However, failure to address a specific rejection, issue or comment, does not signify agreement with or concession of that rejection, issue or comment. In addition, because the arguments made above are not intended to be exhaustive, there may be reasons for patentability of any or all pending claims (or other claims) that have not been expressed. Finally, nothing in this paper should be construed as an intent to concede any issue with regard to any claim, except as specifically stated in this paper, and the amendment of any claim does not necessarily signify concession of unpatentability of the claim prior to its amendment.

For all of these reasons, it is respectfully suggested that all of the claims should be in condition for allowance. A formal notice of allowance is hence respectfully requested.

If the Examiner believes that communications such as a telephone interview or email would facilitate disposal of this case, the undersigned respectfully encourages the Examiner to contact the undersigned.

Recognizing that Internet communications are not secure, I hereby authorize the USPTO to communicate with me concerning any subject matter of this application by electronic mail (using the

email address scott@harrises.com). I understand that a copy of these communications will be made of record in the application file.

Please charge any fees due in connection with this response to Deposit Account No. 50-1387, small entity.

Respectfully submitted,

Date: _9/30/2008_____ __/Scott C Harris/_____
Scott C. Harris
Reg. No. 32,030

Customer No. 23844
Scott C. Harris, Esq.
P.O. Box 927649
San Diego, CA 92192
Telephone: (619) 823-7778
Facsimile: (858) 756-7717

Attachment: SSID document